J. Symbolic Computation (2000) **30**, 239–251
doi:10.1006/jsco.2000.0361
Available online at http://www.idealibrary.com on IDEAL

Computing Local Artin Maps, and Solvability of Norm Equations

VINCENZO ACCIARO[†§] AND JÜRGEN KLÜNERS[‡¶]

[†] *Dipartimento di Informatica, Universita' degli Studi di Bari, via E. Orabona 4, Bari 70125, Italy*
[‡] *Universität Heidelberg, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany*

Let $L = K(\alpha)$ be an Abelian extension of degree n of a number field K, given by the minimal polynomial of α over K. We describe an algorithm for computing the local Artin map associated with the extension L/K at a finite or infinite prime v of K. We apply this algorithm to decide if a nonzero $a \in K$ is a norm from L, assuming that L/K is cyclic.

1. Introduction

The problem of effectively constructing local and global Artin maps was posed in Lenstra (1992). Acciaro and Klüners (1999) have shown how to construct the Artin symbol $(p, L/\mathbb{Q})$ of a rational prime p in $\mathrm{Gal}(L/\mathbb{Q})$, with $L/\mathbb{Q}$ Abelian. Subsequently, the second author has shown (Klüners, 1997) how to extend this algorithm to construct the Artin symbol $(\mathfrak{p}, L/K)$ of a prime $\mathfrak{p}$ of K in $\mathrm{Gal}(L/K)$, where K is an arbitrary number field and L/K is Abelian. In the present paper we exploit this algorithm to construct the local Artin maps associated to an Abelian extension L/K of degree n, where $L = K(\alpha)$ is given by the minimal polynomial $m_\alpha(x)$ of α over K. Although it is possible to define the local Artin map in several ways, we have chosen to use the language of ideles as a convenient tool to describe the effective construction.

We apply this algorithm to solve the following problem: *Let $L = K(\alpha)$ be a cyclic extension of a number field K of degree n, given by the minimal polynomial $m_\alpha(x)$ of α over K, and let $a \in K$, with $a \neq 0$; decide if the equation*

$$N_{L/K}(\lambda) = a \tag{1.1}$$

admits any solution λ in L.

Note that we are not interested in finding a solution λ, but simply in determining whether a solution exists. Without loss of generality we can assume that $\alpha \in \mathcal{O}_L$, the ring of algebraic integers of L. Our algorithm is based on the well-known Hasse Norm Theorem, which states that, for a cyclic extension of number fields, an element of the base field is a global norm if and only if it is a local norm everywhere.

Acciaro (1996) described an algorithm to solve the same problem, assuming that n is

[§] E-mail: acciaro@di.uniba.it
[¶] E-mail: klueners@iwr.uni-heidelberg.de

0747–7171/00/030239 + 13 $35.00/0

prime and K is the field $\mathbb{Q}$ of rationals. In the present paper we remove this constraint, and we use a different technique to attack the problem — namely, by exploiting the local Artin maps associated to the extension L/K.

If we assume that $a \in \mathbb{Z}$, the rational integers, and we ask for solutions of (1.1) in the algebraic integers, we can use an algorithm, due to Fincke and Pohst (Pohst and Zassenhaus, 1989, p. 336), based on methods borrowed from the geometry of numbers, which works for any finite extension of $\mathbb{Q}$. However, even if (1.1) is not solvable in the algebraic integers, it may still be solvable in $\mathbb{Q}(\alpha)$. A generalization of this algorithm to relative extensions is presented in Fieker (1997). In Fieker's thesis there is a different approach to solve norm equations based on the computation of S-units; moreover, it is possible to solve the norm equation in arbitrary orders or in the given field.

The paper is organized as follows. In Section 3.1 we recall the ideal theoretical definition of the Artin map for Abelian extensions of number fields. Then, in Section 3.4 we give the idele theoretical definition. Finally, in Section 3.5 we give the definition of the Artin map for Abelian extensions of local fields, and we show how to compute it. In Section 4 we show how to apply our algorithms to decide if (1.1) is solvable.

The algorithms described in this paper have been implemented using the number theory package KASH (Daberkow *et al.*, 1997), developed in Berlin by Professor Pohst and his collaborators.

For the terminology and the basic concepts of algebraic number theory used in this paper we refer the reader to Lang (1994).

2. Notation

If k is a subfield of a field K, then $[K : k]$ will denote the degree of the field extension K/k, and $K^* = K\backslash\{0\}$ will denote the multiplicative group of K.

Let k be an algebraic number field. The symbol $\mathcal{O}_k$ will denote the ring of integers of k. By a prime of k we mean a class of equivalent valuations of k. Recall that the finite primes are in one-to-one correspondence with the prime ideals of $\mathcal{O}_k$, and the infinite primes are in correspondence with the embeddings of k into $\mathbb{C}$, the field of complex numbers.

The symbols v and w will denote primes of an algebraic number field, either non-archimedean or archimedean.

Let v be a finite prime of k. The symbol k_v will denote the completion of k with respect to the v-adic valuation, and $\mathcal{O}_v$ the corresponding ring of v-adic integers.

Let v be an infinite prime of k, that is, an embedding $v : k \hookrightarrow \mathbb{C}$. The symbol k_v will denote the completion of k with respect to the (archimedean) valuation $\beta \mapsto |v(\beta)|$.

3. Global and Local Artin Maps

3.1. Global Artin maps (ideal approach)

In the following L/K will always be a finite Abelian extension. By $\mathfrak{d}_{L/K}$ we denote the relative discriminant of L/K as an ideal of $\mathcal{O}_K$. Let $\mathfrak{P}$ be an unramified prime ideal of $\mathcal{O}_L$ which lies above a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. We denote by $\sigma_{\mathfrak{P}}$ the Frobenius automorphism of $\mathfrak{P}$. Since L/K is Abelian, this automorphism depends only on $\mathfrak{p}$ and is called the Artin automorphism of $\mathfrak{p}$; it is denoted by $(\mathfrak{p}, L/K)$. The Artin map is the multiplicative

extension of this map to the group of fractional ideals $I^{\mathfrak{d}_{L/K}}$ which are prime to $\mathfrak{d}_{L/K}$:

$$(\cdot, L/K) : I^{\mathfrak{d}_{L/K}} \to \mathrm{Gal}(L/K) : \mathfrak{a} = \prod_{\mathfrak{p}|\mathfrak{a}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} \mapsto \prod_{\mathfrak{p}|\mathfrak{a}} (\mathfrak{p}, L/K)^{v_{\mathfrak{p}}(\mathfrak{a})}.$$

Acciaro and Klüners (1999) have shown how to compute the Artin automorphism of a prime p in the case $K = \mathbb{Q}$. Klüners (1997) has extended this algorithm for arbitrary number fields K. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ which is unramified in L. Let α be a primitive element of L/K. Then we know that the Artin automorphism $(\mathfrak{p}, L/K)$ has the following property:

$$(\mathfrak{p}, L/K)(\alpha) \equiv \alpha^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{p}\mathcal{O}_L \tag{3.1}$$

where N is the norm function applied to ideals giving integers (see Lang, 1994, p. 24, for a definition).

The automorphism $\sigma = (\mathfrak{p}, L/K)$ is determined by $\beta := \sigma(\alpha) = \frac{1}{d}\sum_{i=0}^{n-1} a_i \alpha^i$, where $a_i \in \mathcal{O}_K,\ d \in \mathbb{N}$. Using (3.1) we compute $\beta_1 \equiv \alpha^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{p}\mathcal{O}_L$. Using Newton's algorithm we compute an element $\beta_k \in \mathcal{O}_K[\alpha]$ with

$$\beta_k = \sum_{i=0}^{n-1} a_{i,k}\alpha^i \equiv \beta \bmod \mathfrak{p}^k\mathcal{O}_L$$

for a suitable $k \in \mathbb{N}$. Then we get for $0 \le i < n$:

$$\frac{a_i}{d} \equiv a_{i,k} \bmod \mathfrak{p}^k.$$

In the case $K = \mathbb{Q}$ we can easily derive bounds for d and a_i. Choosing k sufficiently large we can compute a_i and d with an algorithm based on continued fractions (Collins and Encarnación, 1995).

In the case $K \neq \mathbb{Q}$ the reconstruction of a_i and d from $a_{i,k}$ is more complicated. If $\mathfrak{p}$ is the only prime ideal lying over p this process is essentially the same. When $p\mathcal{O}_k = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ $(\mathfrak{p}_1 = \mathfrak{p})$, we use a combinatorial approach to compute $\sigma(\alpha) \bmod \mathfrak{p}_i\mathcal{O}_L$ $(2 \le i \le r)$. Using the Chinese Remainder Theorem we can compute $\sigma(\alpha) \bmod p\mathcal{O}_L$. Again we can use Newton's method to compute $\sigma(\alpha) \bmod p^k\mathcal{O}_L$. Knowing this, the reconstruction process is analoguous to the case $K = \mathbb{Q}$. For more details we refer to Klüners (1997).

3.2. IDELES

Let us first recall some basic facts about the ideles. If v is a finite prime of K, then the symbol U_v will denote the group of units of $\mathcal{O}_v$. If v is an infinite prime of K, then the symbol U_v will denote the multiplicative group K_v^* of the field K_v. Let S be a finite set of primes of K; the group of S-ideles of K is defined to be:

$$\mathbb{J}_K^S = \prod_{v \in S} K_v^* \times \prod_{v \notin S} U_v.$$

The idele group of K is defined to be the union of all the groups $\mathbb{J}_K^S$, where S runs through all finite sets of primes of K.

3.3. ADMISSIBLE CYCLES

A *cycle* (or *modulus*) $\mathfrak{m}$ of an algebraic number field K is a formal finite product of primes (finite or infinite) of K. A finite prime v may occur in $\mathfrak{m}$ with multiplicity ≥ 1. If

v is a real infinite prime, then it may occur in $\mathfrak{m}$ with multiplicity 1. A complex infinite prime must not occur in $\mathfrak{m}$.

The notion of admissible cycle is of great importance in global class field theory. Its definition will not be given here; the interested reader can consult Lang (1994). For our purposes it is enough to recall the following properties:

> An admissible cycle for an Abelian extension L/K of number fields is divisible by all the primes of K which ramify in L;
>
> There is a smallest admissible cycle $\mathfrak{f}$ called the *conductor* of the extension L/K; any admissible cycle $\mathfrak{c}$ for L/K is a multiple of $\mathfrak{f}$;
>
> A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is ramified, if and only if $\mathfrak{p} \mid \mathfrak{f}$. It is wildly ramified, if and only if $\mathfrak{p}^2 \mid \mathfrak{f}$.

Since the relative discriminant $\mathfrak{d}_{L/K}$ of L/K divides the discriminant $\operatorname{disc}(m_\alpha(x))$ of $m_\alpha(x)$, it is easy to obtain an admissible cycle for our extension L/K, as follows.

It is clear that $\operatorname{disc}(m_\alpha(x)) \in \mathcal{O}_K$ since $\alpha \in \mathcal{O}_L$. Let $\mathfrak{c}_0 = \operatorname{disc}(m_\alpha(x))\ \mathcal{O}_K$. Let $\mathfrak{c}_\infty$ be the formal product of the infinite primes of K which ramify in L. Then $\mathfrak{c} = \mathfrak{c}_\infty \mathfrak{c}_0$ is an admissible cycle for L/K.

If we factorize

$$\mathfrak{c}_0 = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i},$$

we can easily obtain a smaller admissible cycle $\mathfrak{c}_\infty \tilde{\mathfrak{c}}_0$, as follows. We denote by p_i the characteristic of the residue class field of $\mathfrak{p}_i$. If $p_i > n$ we know that $\mathfrak{p}_i$ cannot be wildly ramified. We define

$$\tilde{\mathfrak{c}}_0 := \prod_{i=1}^{r_0} \mathfrak{p}_i^{e_i} \prod_{i=r_0+1}^{r} \mathfrak{p}_i,$$

where we assume that $p_i \leq n$ $(1 \leq i \leq r_0)$ and $p_j > n$ $(r_0 < j \leq r)$.

Now we are interested in computing the infinite primes of K which ramify in L. If v is a complex infinite prime it cannot ramify in L. We denote by v a real infinite prime of K. We denote by $\tilde{m}_\alpha \in \mathbb{R}[x]$ the image of m_α under v. The prime v is unramified if all zeros of $\tilde{m}_\alpha$ are in $\mathbb{R}$, otherwise it ramifies. We use Sturm's algorithm (Cohen, 1993, Theorem 4.1.10) for real polynomials to compute the number of real zeros. We remark that for L/K normal we get that this number is equal to 0 or $[L : K]$.

3.4. GLOBAL ARTIN MAPS (IDELE APPROACH)

Let $\mathbb{J}_K$ denote the idele group of K. If $j \in \mathbb{J}_K$ then j_v will denote the local component of j at the prime v (thus $j_v \in K_v^*$), and, as Lang (1994, Chapter 7), we write $j = (j_v)$.

Recall that K^* is embedded in $\mathbb{J}_K$ on the diagonal, by associating with $b \in K^*$ the idele b (there is no risk of confusion, if we adopt the same name) whose vth component is b, for all the primes v of K.

If v is discrete, then we can define the order of j at v to be that integer r_v such that

$$j_v = \pi_v^{r_v} u_v,$$

where π_v denotes a prime element of $\mathcal{O}_v$, the ring of integers of K_v, and u_v some unit of

$\mathcal{O}_v$. Now, by definition of ideles, almost all r_v are equal to 0, and therefore, if we identify a discrete valuation v of K with the corresponding prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the ideal

$$\prod_{\mathfrak{p} \text{ prime ideal of } \mathcal{O}_K} \mathfrak{p}^{r_\mathfrak{p}}$$

is a fractional ideal of K, denoted by (j), and called *the associated ideal* of j.

Let $\mathfrak{c}$ be an admissible cycle for L/K computed in Section 3.3. If $v \mid \mathfrak{c}$ with multiplicity $m(v)$ for some prime v of K, then we define $\mathfrak{c}_v$ to be the ideal generated by $\pi_v^{m(v)}$ in $\mathcal{O}_v$.

If $l \in \mathbb{J}_K$, then we say that $l \equiv 1 (\mathrm{mod}^*\ \mathfrak{c})$ iff for all $v \mid \mathfrak{c}$:

If v is infinite, then $l_v > 0$;
If v is finite, then $l_v \in \mathcal{O}_v$ and $l_v \equiv 1 \pmod{\mathfrak{c}_v}$.

LEMMA 3.1. *Let $\mathfrak{c}$ be an admissible cycle. Then there is an isomorphism*

$$\mathbb{J}_\mathfrak{c}/K_\mathfrak{c} \cong \mathbb{J}_K/K^*$$

where $J_\mathfrak{c} := \{a \in \mathbb{J}_K \mid a \equiv 1 \mod^* \mathfrak{c}\}$ and $K_\mathfrak{c} := J_\mathfrak{c} \cap K^*$.

PROOF. We prove that any idele class (element of $\mathbb{J}_K/K^*$) has a representative idele in $J_\mathfrak{c}$ for any given $\mathfrak{c}$. Given $l \in \mathbb{J}_K$ select $b \in K^*$ using the approximation theorem such that $lb \equiv 1 (\mathrm{mod}^*\ \mathfrak{c})$.

DEFINITION 3.1. Let $\mathfrak{c}$ be a cycle. We denote by $I(\mathfrak{c})$ the group of fractional ideals of o_K, which are prime to $\mathfrak{c}$. $P_\mathfrak{c}$ is the set of principal ideals (a) of $\mathcal{O}_K$ with $a \in K_\mathfrak{c}$. Finally $\Pi(\mathfrak{c}) := \Pi(\mathfrak{c}, L/K) := \{N_{L/K}(\mathcal{A}) \mid \mathcal{A}$ is a fractional ideal of $\mathcal{O}_L$ prime to $\mathfrak{c}\}$.

We can state the following theorem (Lang, 1994, Theorem 8, p. 150).

THEOREM 3.1. *Let L/K be an Abelian extension and $\mathfrak{c}$ be an admissible cycle for L/K. Then we have an isomorphism*

$$\mathbb{J}_K/K^* N_{L/K} \mathbb{J}_L \cong I(\mathfrak{c})/P_\mathfrak{c}\Pi(\mathfrak{c}).$$

The isomorphism is induced by the isomorphism

$$\mathbb{J}_\mathfrak{c}/K_\mathfrak{c} \cong \mathbb{J}_K/K^*,$$

followed by the ideal map $l \mapsto (l)$ of $\mathbb{J}_\mathfrak{c}$ onto $I(\mathfrak{c})$.

Following Lang (1994, Chapter X, Section 3) we can define the Artin map for ideles. Let $l \in \mathbb{J}_K$ be an idele, and let $b \in K^*$ such that $lb \equiv 1 (\mathrm{mod}^*\ \mathfrak{c})$. If $\mathfrak{a}$ is the associated ideal of lb, then $(l, L/K)$ is defined to be $(\mathfrak{a}, L/K)$. This is well defined, since from our definition we get $(b, L/K) = 1$ for all $b \in K^*$.

3.5. LOCAL ARTIN MAPS

It is possible to define in several ways the local Artin map at a prime v associated to an Abelian extension L/K of number fields. Lang, in his approach to Class Field Theory (Lang, 1994, Part Two), goes from the global situation to the local one. In this paper we follow closely Lang's approach.

The objective of Local Class Field Theory is to describe all the Abelian extensions of a local field. We remark that all local fields in this paper are finite extensions of completions of $\mathbb{Q}$. Recall first that the main theorem of Local Class Field Theory establishes a one-to-one correspondence between the Abelian extensions of a local field F and the open subgroups of finite index in F^*. More precisely, for a fixed local field F, to each Abelian extension E of F there corresponds uniquely the norm subgroup $N_{E/F}(E^*)$ of F^*, and conversely, any open subgroup of finite index in F^* is the norm subgroup of some Abelian extension E of F. We have the following theorem (Lang, 1994, Theorem 5, p. 221).

THEOREM 3.2. *For a given Abelian extension E of a local field F, there is a canonical homomorphism:*

$$(\cdot, E/F) : F^* \to \mathrm{Gal}(E/F)$$

called the norm residue symbol*, whose kernel is precisely the norm group $N_{E/F}(E^*)$. The norm residue symbol induces an isomorphism:*

$$F^*/N_{E/F}(E^*) \cong \mathrm{Gal}(E/F)$$

called the main isomorphism of Local Class Field Theory.

Before turning to the construction of the local Artin map associated to an Abelian extension of local fields, recall that if L/K is an Abelian extension of number fields, and w is a prime of L lying above a prime v of K, then L_w/K_v is an Abelian extension of local fields, whose Galois group is isomorphic to the decomposition group of w in $\mathrm{Gal}(L/K)$. Since L/K is Abelian the decomposition group of w is the same for all primes w lying over v.

It is possible to embed K_v^* in $\mathbb{J}_K$ on the vth component, by identifying an element $a_v \in K_v^*$ with the idele $[a_v]$ whose vth component is a_v, and having component 1 at all the other primes of K. Thus, we can consider the local map $(\cdot, L_w/K_v)$ as a restriction to K_v^* of the global Artin map $(\cdot, L/K)$ defined on the idele group of K. The compatibility of the two maps is guaranteed by the following.

THEOREM 3.3. *If L/K is an Abelian extension of number fields, and w is a prime of L lying above a prime v of K, then the diagram*

$$\begin{array}{ccc} K_v^* & \xrightarrow{(\cdot, L_w/K_v)} & \mathrm{Gal}(L_w/K_v) \\ \big\downarrow{\scriptstyle [\cdot]} & & \big\downarrow{\scriptstyle \eta} \\ \mathbb{J}_K & \xrightarrow{(\cdot, L/K)} & \mathrm{Gal}(L/K) \end{array}$$

is commutative, where η denotes the standard embedding of $\mathrm{Gal}(L_w/K_v)$ *into* $\mathrm{Gal}(L/K)$.

PROOF. This is just a restatement of Neukirch (1986, Proposition 6.6, p. 94), using ideles rather then idele classes.

For this reason the norm residue symbol $(\cdot, L_w/K_v) = ([\cdot], L/K)$ is also called local Artin map.

3.6. COMPUTATION OF THE LOCAL NORM RESIDUE SYMBOL

Let $a_v \in K_v^*$; we want to compute $(a_v, L_w/K_v)$. In the following we denote by $m(v)$ the integer such that $\mathfrak{c} = v^{m(v)}\tilde{\mathfrak{c}}$ with $v \nmid \tilde{\mathfrak{c}}$. We proceed as follows.

(i) First, we embed K_v in $\mathbb{J}_K$ by considering the idele j whose vth component is a_v and all the others are equal to 1.
(ii) Using the approximation theorem for Dedekind rings, we find $h \in K^*$ such that:

$$a_v \equiv h \bmod v^s, \text{ where } s = m(v) + \mathrm{ord}_v(a_v) \text{ and}$$
$$h \equiv 1 \bmod^* \tilde{\mathfrak{c}}.$$

(iii) Now, we have $jh^{-1} \equiv 1 (\bmod^* \ \mathfrak{c})$.
(iv) Let $\mathcal{I}$ be the associated ideal of jh^{-1}, and let $\prod_{i=1}^k \mathfrak{p}_i^{s_i}$ be its complete factorization in K.
(v) Next, we compute the Artin automorphism $(\mathcal{I}, L/K)$ of $\mathcal{I}$ by exploiting the multiplicativity of the Artin symbol, that is

$$(\mathcal{I}, L/K) = \prod_{i=1}^{k} (\mathfrak{p}_i, L/K)^{s_i}$$

where the product on the right-hand side is meant to be in $\mathrm{Gal}(L/K)$.
(vi) By Theorem 3.3, we have $(a_v, L_w/K_v) = \eta^{-1}(\mathcal{I}, L/K)$.

3.7. THE UNINTERESTING CASE

The computation of the norm residue symbol is trivial when the local extension L_w/K_v is unramified—in particular, this happens when $v \nmid \mathfrak{c}_0$. In fact, when v is unramified then $\mathrm{Gal}(L_w/K_v)$ is cyclic of order f and it is isomorphic to the decomposition group of L/K at v, which is generated by the (global) Artin map of L/K at v. Let π_v denote a prime element of K_v, and $\mathfrak{p}$ the prime ideal of $\mathcal{O}_K$ corresponding to v. Now, if we write an element a_v of K_v as

$$a_v = \pi_v^{\mathrm{ord}_v(a_v)} \ u_v$$

for some v-adic unit u_v, it is clear that

$$(a_v, L_w/K_v) = \eta^{-1}(\mathfrak{p}, L/K)^{\mathrm{ord}_v(a_v)}. \tag{3.2}$$

3.8. THE ALGORITHM

Now we are able to give the algorithm to compute the local Artin map $(a_v, L_w/K_v)$ for an element $a_v \in K_v^*$. As before we denote by $m(v)$ the integer such that $\mathfrak{c} = v^{m(v)}\tilde{\mathfrak{c}}$ with $v\tilde{\mathfrak{c}}$.

We can represent an element a_v of K_v as a convergent series, in the v-adic topology:

$$a_v = \sum_{i=\mathrm{ord}_v(a_v)}^{\infty} c_i \ \pi_v^i$$

where π_v denotes a prime element of K_v, and the elements c_i are taken from a fixed set of coset representatives of the residue class field. Without loss of generality, we can assume

that $\pi_v, c_i \in K$. It will be clear from the description of the algorithm that we need only to consider the (finite) approximation:

$$\sum_{i=\mathrm{ord}_v(a_v)}^{s} c_i\ \pi_v^i$$

for $s = m(v) + \mathrm{ord}_v(a_v)$.

ALGORITHM 3.1. (Computation of the local Artin map at a finite prime v)

Input: *An Abelian extension L/K, a finite valuation v, a finite approximation $\sum_{i=\mathrm{ord}_v(a_v)}^{s} c_i\ \pi_v^i$ of $a_v \in K_v^*$, where $s = m(v) + \mathrm{ord}_v(a_v)$.*

Output: $(a_v, L_w/K_v)$.

Step 1: *Compute the automorphism group of L/K.*

Step 2: *Compute an admissible cycle $\mathfrak{c}$ of L/K.*

Step 3: *If $v \nmid \mathfrak{c}$ then return $(\mathfrak{p}, L/K)^{\mathrm{ord}_v(a_v)}$, where $\mathfrak{p}$ is the corresponding prime ideal to v.*

Step 4: *Let $h_1 = \sum_{i=\mathrm{ord}_v(a_v)}^{s-1} c_i\ \pi_v^i$, with $s = m(v) + \mathrm{ord}_v(a_v)$.*

Step 5: *Find an element $h \in K$ such that $h \equiv h_1 \bmod v^s$ and $h \equiv 1 \bmod^* \tilde{\mathfrak{c}}$, using the approximation theorem.*

Step 6: *Set $\mathfrak{a} := h\ \mathfrak{p}^{-\mathrm{ord}_v(h)}$.*

Step 7: *Return $(\mathfrak{a}, L/K)^{(-1)}$.*

PROOF. Write $\mathfrak{c}$ as $v^{m(v)}\tilde{\mathfrak{c}}$, with $v \nmid \tilde{\mathfrak{c}}$. By construction, we have that

$$a_{v'}h^{-1} \equiv 1 \bmod v^{m(v)} \tag{3.3}$$

for each $v' \neq v$ and $v' \mid \mathfrak{c}$, since $a_{v'}$ in this case is defined to be 1 (note for the reader: $a_{v'}$ is the component of the idele $[a_v]$ at the prime v', which is equal to 1).

Let $s = m(v) + \mathrm{ord}_v(a_v)$. By construction, we have that $h_1 \equiv a_v \bmod v^s$, and hence $h \equiv a_v \bmod v^s$, as well. Therefore

$$a_v h^{-1} \equiv 1 \bmod v^{m(v)}. \tag{3.4}$$

Now, (3.3) and (3.4) imply that

$$a_v h^{-1} \equiv 1 \bmod \tilde{\mathfrak{c}}.$$

We remark that in Step 5 of the above algorithm the infinite primes are important. For the algorithmic solution of this step we need a generalization of the Chinese Remainder Theorem. Let $\tilde{\mathfrak{c}} = \tilde{\mathfrak{c}}_0\mathfrak{c}_\infty$, where $\tilde{\mathfrak{c}}_0$ is a product of finite primes. In the case $K = \mathbb{Q}$ we simply choose an element $h \in \mathbb{Q}$ such that

$$h \equiv h_1 \bmod v^s,\ h \equiv 1 \bmod^* \tilde{\mathfrak{c}_0} \text{ and } h > 0.$$

In the general case we use the function *RayCantoneseRemainder* of KASH (Daberkow *et al.*, 1997) which is described in Pauli and Pohst (1997). We give a simple solution to this problem:

(i) Compute $h \in K$ such that $h \equiv h_1 \bmod v^s$ and $h \equiv 1 \bmod^* \tilde{\mathfrak{c}_0}$.
(ii) Compute the minimal natural number m in the ideal $\mathfrak{c}_0 v^s$.
(iii) While $h \not\equiv 1 \bmod^* \mathfrak{c}_\infty$ set $h := h + m$.
(iv) Return h.

This algorithm terminates after a finite number of steps with the correct result. Now we give an algorithm to compute the local Artin symbol for an infinite prime. We remark that it is easier to decide if the Artin symbol is the identity than to compute it.

ALGORITHM 3.2. (Computation of the local Artin map at an infinite prime v)

Input: *An Abelian extension L/K, an admissible cycle $\mathfrak{c}$ of L/K, an infinite valuation v, and $a_v \in K_v$.*

Output: $(a_v, L_w/K_v)$.

Step 1: *If v is complex or $a_v > 0$ then return the identity.*

Step 2: *If $v \nmid \mathfrak{c}$ then return the identity.*

Step 3: *Compute $h \in K$ such that $h \equiv 1 \bmod^* \tilde{\mathfrak{c}}$ and $h \not\equiv 1 \bmod^* v$ using the approximation theorem.*

Step 4: *Set $\mathfrak{a} := h\mathcal{O}_K$.*

Step 5: *Return $(\mathfrak{a}, L/K)$.*

4. Application: Solvability of Norm Equations

The following theorem (Neukirch, 1986, Corollary 5.2, p. 89) is fundamental to this section.

THEOREM 4.1. (HASSE NORM THEOREM) *Let L/K be a cyclic extension of number fields. An element $a \in L^*$ is a norm from L^* if and only if a is a local norm at every prime (including the infinite primes) of L.*

We will deal with the infinite primes in Section 4.4. Until then, all the primes considered will be finite.

Recall that the property of being Galois is preserved by the completions at the finite primes. In fact, if L is a finite Galois extension of an algebraic number field K, and w is a prime of L lying above a prime v of K, then L_w/K_v is also Galois, with Galois group equal to the decomposition group G_w of w.

Throughout the following, L will denote a cyclic extension of degree n of K.

4.1. DECOMPOSITION OF PRIMES NOT DIVIDING $\mathfrak{c}$

Our first task is to recognize the residue degree f of a finite prime $v \nmid \mathfrak{c}$. We suppose that v does not divide $\mathrm{disc}(\alpha)\mathcal{O}_K$, otherwise we use the admissible cycle $v\mathfrak{c}$ instead of $\mathfrak{c}$.

We compute

$$\bar{\beta} := \alpha^{\mathrm{N}(v)} = \sum_{i=0}^{n-1} (a_i \bmod v)\alpha^i,$$

where $a_i \bmod v$ is the unique representative computed with (Cohen, 1996, Algorithm 2.11). Using the same algorithm we compute $\bar{\beta}_i := \sigma_i(\alpha) \bmod v\mathcal{O}_L$ $(1 \le i \le n)$. This is not a problem, since the automorphisms $\sigma_1, \ldots, \sigma_n$ of L/K are known at this point. After this, we simply compare $\bar{\beta}$ with $\bar{\beta}_i$ to determine the Frobenius automorphism of v. The residue degree is equal to the order of the corresponding σ_i. Another possibility for determining the residue degree of v is to compute the smallest number f such that $\alpha^{\mathrm{N}(v)^f} \equiv 1 \bmod v$.

4.2. THE UNRAMIFIED CASE

In this section we assume that the finite prime v does not divide $\mathfrak{c}$: it follows that v is certainly unramified in L.

The case when $f = 1$, that is, when v *splits completely* in L, is uninteresting, since we have $L_w = K_v$, and so any $a \in K_v^*$ is the norm of itself in the trivial extension of K_v.

Hence we will restrict our attention to the case $f > 1$. Then L_w is an unramified extension of K_v of degree f, and the next theorem characterizes completely the norm group of L_w/K_v.

THEOREM 4.2. *Let L_w be an unramified extension of K_v of degree f. Let $\beta = \pi_v^m\, u_v \in K_v^*$, with u_v a unit in $\mathcal{O}_v$, $m \in \mathbb{Z}$. Then $\beta \in N_{L_w/K_v}(L_w^*)$ if and only if $f \mid m$. In particular, every unit of $\mathcal{O}_v$ is the norm of a unit in L_w.*

PROOF. The proof follows easily from (3.2) and Theorem 3.2.

Therefore in our case, if m denotes the order of a at v, then a is a local norm at v iff $f \mid m$. This implies in particular that the only finite unramified primes which must be taken into account are those involving the factorization of a, and clearly there is only a finite number of them.

4.3. THE (POSSIBLY) RAMIFIED CASE

In this section we assume that the finite prime v of K divides $\mathfrak{c}$: it follows that v might ramify in L. However, we are not interested in deciding whether v does ramify or not in L. Let w be *any* prime of L lying above v. By Theorem 3.2 we know that $a \in N_w(L_w^*)$ iff $(a, L_w/K_v)$ is the identity in $\mathrm{Gal}(L_w/K_v)$, and we know how to compute $(a, L_w/K_v)$.

4.4. THE INFINITE PRIMES

Since $L = K(\alpha)$ is Galois over K, if we fix a prime (finite or infinite) v of K, then the Galois group $\mathrm{Gal}(L/K)$ permutes transitively the primes w of L lying above v.

If $K_v = \mathbb{C}$, then L_w must be $\mathbb{C}$ as well, and any element of $\mathbb{C}$ is the norm of itself in the trivial extension of $\mathbb{C}$.

If $K_v = \mathbb{R}$ and $L_w = \mathbb{R}$, then again any element of $\mathbb{R}$ is the norm of itself in the trivial extension of $\mathbb{R}$.

Therefore we have to take into account only the infinite primes v of K which ramify in L, that is those v dividing $\mathfrak{c}_\infty$. In this case we have $N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}) = \mathbb{R}^+$, the nonnegative reals.

Since all the primes w of L lying above an infinite prime v of K are conjugate, we obtain in this way a simple criterion to decide if a is a local norm at each infinite prime. We have to consider only the sign of a at each ramified infinite prime of K (read: at each ramified embedding of K in $\mathbb{C}$).

4.5. THE ALGORITHM

Now we are able to give the whole algorithm to decide if a norm equation of a cyclic extension has a solution.

ALGORITHM 4.1. (NormSolvable)

Input: *A cyclic extension L/K, $a \in K^*$.*

Output: *True, if there exists $\lambda \in L$ with $\mathrm{N}_{L/K}(\lambda) = a$, otherwise false.*

Step 1: *Compute the automorphism group of L/K.*

Step 2: *Compute an admissible cycle $\mathfrak{c}$ of L/K and all v dividing $\mathfrak{c}$.*

Step 3: *Compute a factorization of the ideal $a\mathcal{O}_K$.*

Step 4: *For all finite v with $\mathrm{ord}_v(a) > 0$ or $v \mid \mathfrak{c}$ do:*

1 Compute $(a_v, L_w/K_v)$ using Algorithm 3.1.
2 If $(a_v, L_w/K_v)$ is not the identity, then return false.

Step 5: *If for any ramified infinite prime v we have $a_v < 0$ then return false.*

Step 6: *Return true.*

The correctness of the algorithm follows immediately from Theorem 3.2. We remark that in Step 5 it is necessary that we only consider infinite primes which are ramified. If we do not want to compute the ramification at the infinite primes, we can put all infinite real primes in $\mathfrak{c}$. In this case we have to use Algorithm 3.2 instead of the test $a_v < 0$ in Step 5.

5. Examples

In this section we give some examples to demonstrate the efficiency of our algorithm. All computations were done on a Sun-Ultra-2 300 MHz using KASH 1.9 under SunOS 5.6.

We compare our function for determining the solvability of norm equations with the function *OrderNormEquation* in KASH (Daberkow *et al.*, 1997) which is based on the algorithm of Fincke and Pohst (Pohst and Zassenhaus, 1989). The comparison is unfair

Table 1.

Norms	Number of solvable equations	Time Norm-Solvable k	Time Order-NormEquation	Time combination
1, ...,100	12	0.1 s	13.3 s	1.1 s
1001, ..., 1100	7	0.2 s	166 s	0.5 s
10001, ..., 10100	6	0.3 s	1741 s	1.8 s
100001, ..., 100100	5	0.4 s	8 h	11 s

Table 2.

Norms	Number of solvable equations	Time Norm-Solvable	Time combination
$(\beta+1), \ldots, (\beta+10)$	1	0.8 s	2.6 s
$(\beta^2+1), \ldots, (\beta^2+10)$	3	1.1 s	33.3 s
$(\beta^2+\beta+1), \ldots, (\beta^2+\beta+10)$	4	1.0	46 s

since the output of the two functions is different. The first function determines whether a solution exists, while the second one computes it. Another difference is that our algorithm decides whether there is a solution in the extension field, while the second algorithm searches only for a solution in the given order. Very often it occurs that the norm equation has no solution—in this case the output of both algorithms is the same.

We start with a simple example. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^4 + x^3 + x^2 + x + 1$. It is well known that $\mathcal{O}_L = \mathbb{Z}[\alpha]$. Since $\mathcal{O}_L$ is a prinicipal ideal domain we know that there is a solution of the norm equation in L if and only if there is a solution of the norm equation in $\mathcal{O}_L$. In Table 1 we solve the norm equations for the norms given in the column *norms*. We give the whole computing time for the functions *NormSolvable* and *OrderNormEquation*. We give the number of equations which have a solution in L. In the column *combination* we give the computing time for a combined algorithm. We first check if a solution exists. Only in the case where a solution exists do we call *OrderNormEquation* to compute a solution. We have neglected the computing time for the computation of the automorphism group of L/K (0.1 s) and the computation of the unit group (0.3 s).

We can see that the function *NormSolvable* is very efficient in practice. From the timings we can also see that the function *OrderNormEquation* is more efficient if a solution exists—one reason is that the algorithm can stop when a solution is found.

Next, let us consider a relative extension. Let β be a zero of $x^3 - 2$ and $K = \mathbb{Q}(\beta)$. Let $L = K(\alpha)$, where α is a root of $x^4 - 4x^2 + 4 + 2\beta - 2\beta^2$. We remark that L is a subfield of the ray class field of the modulus $8\mathcal{O}_K$. The function *OrderNormEquation* is based on an algorithm described in Fieker (1997). In Table 2 we ignore 50 s of computing time which are only needed for solving the first norm equation. The computation of the automorphism group took 0.6 s.

The following polynomial has cyclic Galois group of order 12 over $\mathbb{Q}(x)$: $y^{12} + 15xy^{11} + (90x^2 - 54)y^{10} + (274x^3 - 645x)y^9 + (441x^4 - 2994x^2 + 921)y^8 + (351x^5 - 6756x^3 + 8490x)y^7 + (108x^6 - 7536x^4 + 29055x^2 - 6336)y^6 + (-3699x^5 + 45057x^3 - 42396x)y^5 +$

Table 3.

X	Norms	Number of solvable equations	Time	Automorphism time
1	1, ..., 100	5	10.5 s	0.2 s
1	100001, ..., 100100	0	11.0 s	
2	1, ..., 100	1	17.7 s	0.3 s
2	100001, ..., 100100	0	15.3 s	
4	1, ..., 100	3	72.9 s	0.4 s
4	100001, ..., 100100	0	66.5 s	
5	1, ..., 100	2	19.2 s	0.3 s
5	100001, ..., 100100	0	18.2 s	
6	1, ..., 100	2	15.8 s	0.4 s
6	100001, ..., 100100	0	10.8 s	
7	1, ..., 100	2	18.8 s	0.3 s
7	100001, ..., 100100	0	17.6 s	

$(-540x^6 + 30777x^4 - 97749x^2 + 16392)y^4 + (7740x^5 - 90412x^3 + 70296x)y^3 + (432x^6 - 31764x^4 + 89940x^2 - 7200)y^2 + (-2880x^5 + 41568x^3 - 12576x)y + 4800x^4 - 6672x^2 + 784$.

In Table 3 we specialize x and obtain polynomials in $\mathbb{Z}[y]$. We give the computing times for *NormSolvable*. The last column gives the time needed for the computation of the automorphism group, which is not included in the computing time for *NormSolvable*.

We remark that specializing $x = 3$ yields a reducible polynomial. The different computing times are due to the different steps at which the algorithm can decide whether the given norm equation is solvable or not. It is much cheaper when an unramified prime indicates that the norm equation is not solvable.

We remark that the most expensive step of the algorithm is the factorization of $\mathfrak{a}$ in Step 7 of Algorithm 3.1. In the last example there are subfields of coprime degree which generate the given field. In this case the norm equation is solvable if and only if the norm equation is solvable for these subfields. Using this fact the computing time can be improved by applying the algorithm to the degree 3 and degree 4 subfields.

Acknowledgment

The first author wishes to thank Professor V. L. Plantamura for his constant support.

References

Acciaro, V. (1996). Solvability of norm equations over cyclic number fields of prime degree. *Math. Comp.*, **65**, 1663–1674.

Acciaro, V., Klüners, J. (1999). Computing automorphisms of Abelian number fields. *Math. Comput.*, **68**, 1179–1186.

Cohen, H. (1993). *A Course in Computational Algebraic Number Theory*, Berlin, Springer.

Cohen, H. (1996). Hermite and smith normal form algorithms over dedekind domains. *Math. Comp.*, **65**, 1681–1699.

Collins, G., Encarnación, M. (1995). Efficient rational number reconstruction. *J. Symb. Comput.*, **20**, 287–297.

Daberkow, M., Fieker, C., Klüners, J., Pohst, M., Roegner, K., Wildanger, K. (1997). KANT V4. *J. Symb. Comput.*, **24**, 267–283.

Fieker, C. (1997). Über relative Normgleichungen in algebraischen Zahl-körpern. Dissertation, Technische Universität at Berlin.
Lenstra, H. W. (1992). Algorithms in algebraic number theory. *Bull. Amer. Math. Soc.*, **26**, 211–244.
Klüners, J. (1997). Über die Berechnung von Automorphismen und Teilkörpern algebraischer Zahlkörper. Dissertation, Technische Universität at Berlin, Berlin.
Lang, S. (1994). *Algebraic Number Theory,* volume 110 of *Graduate Texts in Mathematics*, Springer.
Neukirch, J. (1986). *Class Field Theory*, Berlin, Springer.
Pauli, S., Pohst, M. E. (1997). On the computation of the multiplicative group of residue class rings. Preprint. Technical University of Berlin.
Pohst, M. E., Zassenhaus, H. (1989). *Algorithmic Algebraic Number Theory, Encyclopaedia of mathematics and its applications*, Cambridge University Press.

Originally Received 15 October 1998
Accepted 18 February 2000